DATE(S) ISSUED:

04/08/2014

SUBJECT:

Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (MS14-019)

EXECUTIVE SUMMARY:

A remote code execution vulnerability exists in the way that Microsoft Windows processes .bat and .cmd files that are run from an external network. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

THREAT INTELLIGENCE:

This vulnerability has been publicly disclosed.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1

RISK:

Government:

·	Large and medium government entities: **High**
·	Small government entities: **High**

Businesses:

·	Large and medium business entities: **High**
·	Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A remote code execution vulnerability exists in the way that Microsoft Windows processes .bat and .cmd files that are run from an external network. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

To attempt to exploit this vulnerability an attacker would have to convince a user to browse to a trusted or semi-trusted network location wherein the attacker had placed malicious .bat and .cmd files. The attacker would need to convince the user to run these specially crafted files from the network location for the vulnerability to be exploited. If the network location is external, the network would have to allow SMB traffic outbound through their perimeter filtering device. An attacker would have no way to force users to visit a network location or run specially crafted .bat or .cmd files. Instead, an attacker would have to convince users to take such action. For example, an attacker could trick users into clicking a link that takes them to the location of the attacker's specially crafted files and subsequently convince them to run them.

RECOMMENDATIONS:

The following actions should be taken:

·	Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
·	Do not allow outbound SMB traffic through the network perimeter.

·	Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
·	Remind users not to download, accept, or execute files from un-trusted or unknown sources.
·	Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/security/bulletin/ms14-019

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0315